

Configuração de VLANs

Cisco Packet Tracer

Autor

Eduardo Ferreira de Paula

ferreira.eduardop30@gmail.com

[linkedin.com/in/eduardo-ferreira-de-paula1](https://www.linkedin.com/in/eduardo-ferreira-de-paula1)

DESCRIÇÃO

Este projeto tem como objetivo a criação de uma rede segmentada com VLANs para diferentes tipos de usuários (Alunos, Funcionários e Convidados), utilizando 3 switches L2 (Layer 2). A implementação foi realizada no Cisco Packet Tracer como um estudo do curso técnico em Redes de Computadores, seguindo os conceitos da certificação Cisco CCNA.

Uma VLAN (Virtual Local Area Network) é uma rede lógica que agrupa dispositivos de forma virtual, mesmo que estejam fisicamente conectados em switches diferentes. Ela permite segmentar a rede em domínios de broadcast distintos, melhorando a segurança, o desempenho e a organização da infraestrutura.

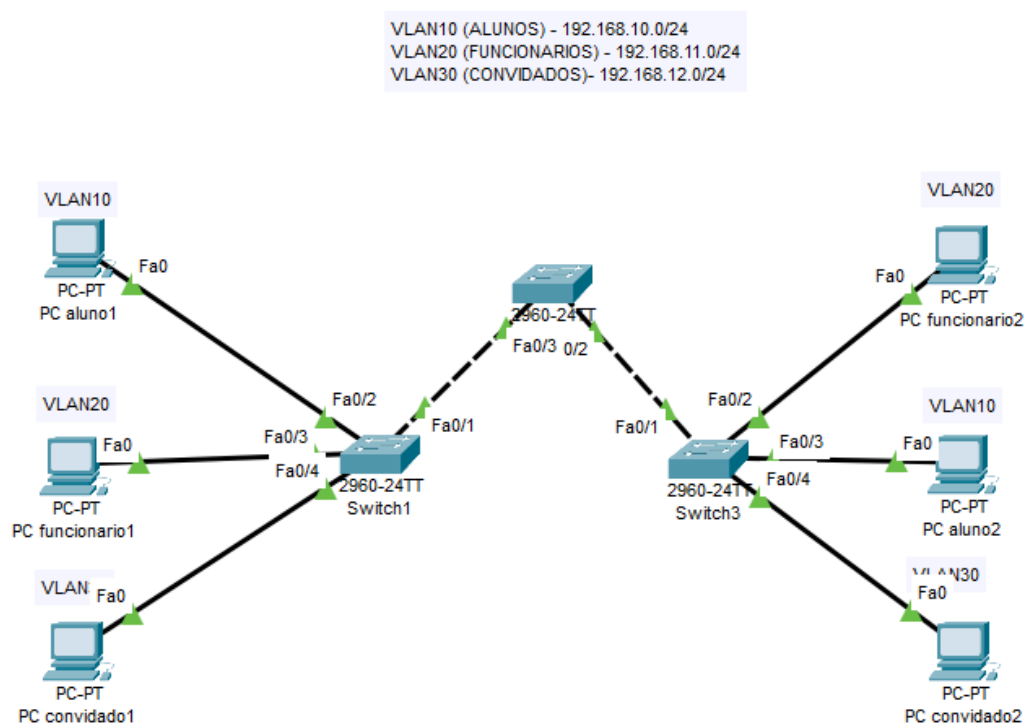
Por padrão, dispositivos em VLANs diferentes não se comunicam entre si. Para permitir essa comunicação, é necessário configurar o roteamento inter-VLAN, utilizando um roteador ou um switch camada 3. Isso garante que cada grupo tenha sua rede isolada, mas com possibilidade de acesso controlado entre elas, conforme as políticas da organização.

Além disso, foi utilizada a configuração de interfaces trunk nos switches, que permitem o tráfego simultâneo de múltiplas VLANs por um único link físico. Essa configuração é fundamental para a comunicação entre switches e entre switch e roteador, pois garante que os quadros de diferentes VLANs sejam transportados corretamente através das interfaces tronco, utilizando o protocolo 802.1Q para identificação das VLANs nos pacotes.

OBJETIVO

- Realizar configuração básica de todos os dispositivos
 - Segmentar a rede local com VLANs
 - Implementar configuração básica em todos dispositivos
 - Isolar as VLANs uma das outras
 - Configurar entrocamento entre os Switches
 - Configurar interfaces de acesso
 - Verificar a comunicação entre hosts da mesma VLAN
 - Verificar a comunicação entre hosts de VLANs diferentes
-

TOPOLOGIA LÓGICA



A rede foi projetada em um modelo de campus simples com três VLANs principais:

- **VLAN10 (ALUNOS)** – 192.168.10.0/24
- **VLAN20 (FUNCIONÁRIOS)** – 192.168.11.0/24
- **VLAN30 (CONVIDADOS)** – 192.168.12.0/24

Dispositivos

- 3 Switches L2
- 6 PCs (2 em cada VLAN)

Conexões

- Cabo Ethernet Direto entre PC e switch
 - Cabo Cross-over entre conexões de switch
 - Interfaces configuradas como trunk entre conexões de switch
 - Switch com portas atribuídas às VLANs específicas
-

ENDEREÇAMENTO IP

VLAN	SUB-REDE	DISPOSITIVO	IP DO DISPOSITIVO
VLAN10 (ALUNOS)	192.168.10.0/24	PC aluno1 PC aluno2	192.168.10.2/24 192.168.10.3/24
VLAN20 (FUNCIONARIOS)	192.168.11.0/24	PC funcionario1 PC funcionario2	192.168.11.2/24 192.168.11.3/24
VLAN30 (CONVIDADOS)	192.168.12.0/24	PC convidado1 PC convidado2	192.168.12.2/24 192.168.12.3/24

CONFIGURAÇÕES REALIZADAS

Realiza a configuração essencial para todos os Switches, como nome, senhas, banners e etc.

Configurações comuns (TODOS SWITCHES)

hostname (nome_de_cada_switch)

Definição de senha privilegiada (enable)

enable secret cisco

Banner de aviso

banner motd #SOMENTE AUTORIZADOS#

Senha no console

line con 0

password cisco

login

Senha nas linhas VTY (acesso remoto)

line vty 0 4

password cisco

login

Configuração das VLANs

vlan 10

name ALUNOS

vlan 20

name FUNCIONARIOS

vlan 30


name CONVIDADOS

Criptografia de todas as senhas

service password-encryption

Salvamento das configurações

copy running-config startup-config

 Nota: As senhas utilizadas neste projeto, como “**cisco**”, foram definidas apenas para fins de demonstração e ambiente de laboratório. Em ambientes reais,

recomenda-se o uso de senhas fortes, únicas e com políticas de segurança adequadas.

Configuração Específica

Realiza a configuração de VLANs nos Switches

(SWITCH2)

Configuração das portas trunk para transporte das VLANs 10, 20 e 30

```
int range fa0/2 - 3
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 10,20,30
```

(SWITCH1)

Portas Access

```
int range fa0/2 - 4
```

```
switchport mode access
```

```
int fa0/2
```

```
switchport access vlan 10
```

```
int fa0/3
```

```
switchport access vlan 20
```

```
int fa0/4
```

```
switchport access vlan 30
```

(SWITCH3)

Portas Access

```
int range fa0/2 - 4
```

```
switchport mode access
```

```
int fa0/2
```

```
switchport access vlan 20
```

```
int fa0/3
```

```
switchport access vlan 10
```

```
int fa0/4
```

```
switchport access vlan 30
```

TESTES DE CONECTIVIDADE

Após a implementação da topologia, foram realizados testes de conectividade com o objetivo de validar o correto funcionamento da rede segmentada com VLANs. Os testes visam garantir que as VLANs foram devidamente criadas, atribuídas às interfaces corretas e propagadas entre os switches por meio de links trunk.

Também foi verificada a comunicação entre hosts da mesma VLAN e entre VLANs diferentes.

Esses testes são essenciais para assegurar que os dispositivos estão corretamente configurados, que a segmentação lógica da rede está funcionando conforme o planejado e que a comunicação entre os diferentes segmentos de rede ocorre de forma segura e eficiente.

Segmentação da rede local com VLANs

É necessário verificar se as VLANs foram corretamente criadas e identificadas em cada switch utilizando *show vlan brief*. A criação e nomeação correta das VLANs são fundamentais para a segmentação lógica da rede e o controle do tráfego.

```
SWITCH1#sh vl br
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	ALUNOS	active	Fa0/2
20	FUNCIONARIOS	active	Fa0/3
30	CONVIDADOS	active	Fa0/4
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SWITCH1#
```

Verificação dos Troncos (trunk)

O comando *show interfaces trunk* mostra quais interfaces estão operando em modo trunk, quais VLANs estão permitidas em cada link e qual protocolo de encapsulamento está sendo utilizado. Conforme neste exemplo utilizando o SWITCH2 configurado, as interfaces fa0/2 e fa0/3 estão operando em modo “Trunk”.

```

SWITCH2#sh int trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/2     on        802.1q         trunking    1
Fa0/3     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/2     10,20,30
Fa0/3     10,20,30

Port      Vlans allowed and active in management domain
Fa0/2     10,20,30
Fa0/3     10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2     10,20,30
Fa0/3     10,20,30

SWITCH2#
SWITCH2#

```

Verificação das portas de acesso (portas access)

As interfaces de acesso, ou portas access, são portas de switch configuradas para pertencer a apenas uma única VLAN. Elas são utilizadas para conectar dispositivos finais como PCs, impressoras e servidores, garantindo que cada equipamento esteja vinculado corretamente à VLAN que representa seu grupo ou departamento na rede.

Iremos analisar todas as interfaces “access” deste laboratório utilizando:

show interfaces fa0/2 switchport

show interfaces fa0/3 switchport

show interfaces fa0/4 switchport

Este teste verifica se as portas access estão configuradas no modo correto (access) e se estão associadas à VLAN correspondente (por exemplo, VLAN10 para Alunos, VLAN20 para Funcionários, etc.). Isso garante que os dispositivos sejam inseridos nos domínios de broadcast corretos.

Na imagem abaixo, foi utilizado o comando *show interfaces fa0/2 switchport* no SWITCH3. Conforme a topologia e configuração da rede, a interface fa0/2 está ligada à VLAN20 (Funcionários).

```

SWITCH3#sh int fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (FUNCIONARIOS)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001

```

Comunicação entre hosts da mesma VLAN

Testar a comunicação entre dois dispositivos pertencentes à mesma VLAN, ainda que conectados a switches diferentes. A troca de pacotes entre hosts da mesma sub-rede deve ocorrer normalmente.

- *ping* de um host da VLAN10 para outro host da VLAN10
- Repetir para VLAN20 e VLAN30

Ping do PC aluno1 para o PC aluno2, ambos na VLAN10

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Ping do PC funcionario1 para o PC funcionario2, ambos na VLAN20

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.3

Pinging 192.168.11.3 with 32 bytes of data:

Reply from 192.168.11.3: bytes=32 time<1ms TTL=128
Reply from 192.168.11.3: bytes=32 time<1ms TTL=128
Reply from 192.168.11.3: bytes=32 time<1ms TTL=128
Reply from 192.168.11.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```


Ping do PC convidado1 para o PC convidado2, ambos na VLAN30

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.12.3

Pinging 192.168.12.3 with 32 bytes of data:

Reply from 192.168.12.3: bytes=32 time<1ms TTL=128
Reply from 192.168.12.3: bytes=32 time<1ms TTL=128
Reply from 192.168.12.3: bytes=32 time<1ms TTL=128
Reply from 192.168.12.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

Comunicação entre hosts de VLANs diferentes

Neste teste, vamos verificar se a segmentação de rede por VLAN está funcionando corretamente, impedindo a comunicação direta entre hosts pertencentes a VLANs diferentes em um ambiente com switches de camada 2, sem roteamento inter-VLAN.

O teste consiste em tentar estabelecer comunicação entre hosts localizados em VLANs distintas, utilizando o comando ping. Como não há roteador ou switch de camada 3 configurado, espera-se que não haja resposta, confirmando que o isolamento entre as VLANs está efetivo.

Os pacotes ICMP devem falhar, sem resposta, comprovando que não há comunicação entre as VLANs. Esse comportamento confirma que o isolamento lógico está funcionando como projetado, garantindo segurança e segmentação de tráfego na rede.

Ping do PC aluno1 (VLAN10) para o PC funcionario2 (VLAN20).

```
C:\>ping 192.168.11.3

Pinging 192.168.11.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.11.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

Ping do PC funcionario1 (VLAN20) para o PC convidado2 (VLAN30)

```
C:\>ping 192.168.12.3

Pinging 192.168.12.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.12.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

São Paulo - SP, Julho de 2025